AF
JJW

# IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
# BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

*In re* Patent Application of: Docket No.: P10149

Neal C. Oliver

Serial No.: 09/750,227 Group Art Unit: 2131

Filed: December 29, 2000 Examiner: Jenise E. Jackson

For: **SYSTEM AND METHOD FOR PROVIDING AUTHENTICATION AND VERIFICATION SERVICES IN AN ENHANCED MEDIA GATEWAY**

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**APPEAL BRIEF UNDER 37 C.F.R. §41.37 (a)**

Sir:

Appellants have filed a timely Notice of Appeal from the Final Office Action, on May 24, 2005. A single copy of this brief is provided pursuant to 35 U.S.C. § 41.37(a).

A check for $500.00 to cover the fee for filing this appeal brief is attached hereto. If additional extensions of time are necessary, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefore (including any additional fees for filing of the Appeal Brief) are hereby authorized to be charged, or overpayment credited, to Intel Deposit Account 50-0221.

## REAL PARTY IN INTEREST

The real party in interest in this appeal is Intel Corporation, assignee of the entire interest in the above-identified application.

## RELATED APPEALS AND INTERFERENCES

The Appellants, their legal representatives and the Assignee are not currently aware of any appeal that may directly affect or be indirectly affected by or have some bearing on the Board's decision in this appeal. Attached hereto is a Related Proceedings Appendix showing no related appeals or interferences.

## STATUS OF THE CLAIMS

Claims 1 - 20 are currently pending.

Claims 21-47 have been cancelled.

Claims 1 - 20 and are the subject of this appeal.

No claims have been withdrawn or allowed. The claims in issue are attached in the "Claims Appendix" attached herewith.

## STATUS OF AMENDMENTS

The Advisory Action mailed on June 16, 2005 indicates that the Response Under 37 C.F.R. §1.116 filed on April 22, 2005 will NOT be entered upon filing a Notice of Appeal. However, this is believed to be an error since no amendments to the claims or specification were made in that response.

Thus, it is believed that all prior amendments to the application have been entered.

## SUMMARY OF CLAIMED SUBJECT MATTER

Briefly, embodiments of the present invention are generally directed to systems and methods for authenticating the identity of a second user or caller to a first caller conversing on telephone through a media gateway. As discussed for example on page 27, lines 17-20, embodiments of the present invention are used for "enabling the provision of authentication or identification services to an end-user regarding a caller during or on a call" (emphasis added). As further discussed, for example at page 29, lines 1-4, "...the client device 28 receives a request to "remote authenticate". For example, the request may be initiated by the Authenticator invoking the authentication feature on his/her client device, such as by speaking a voice command or dialog command into a dialog system or a dialog management module" (emphasis added).

Thus, according to embodiments, a caller, during a call, may authenticate the caller on the other end of the line simply be speaking a voice command during the call.

***Independent Claim 1***

The invention recited by claim 1 is directed to a method for providing authentication or identification services to a first user regarding a second user, the method comprising:

establishing a telephone call between the first user and the second user through a media gateway **(page 28, lines 15-20; Figure 12, items 28 and 30)**;

detecting a voice command from the first caller during the telephone call **(page 29, lines 1-4; Figure 12, item 34)**;

requesting a certificate corresponding to the second user from an authentication server in response to the voice command **(page 29, lines 10 et seq.; Figure 12, item 204)**;

returning the certificate corresponding to the second user **(page 29, line 13 et seq.)**;

requesting authentication of the certificate corresponding to the second user from a control program associated with the second user **(page 29, line 14 et seq.)**;

returning an authentication certificate from the control program associated with the second user **(page 29, lines 15 et seq.)** ; and

verifying authentication by comparing the authentication certificate corresponding to the second user and received from the control program associated with the second user with the certificate received from the authentication server **(page 29, lines 18 et seq. Figue12, item 208)**.

***Independent Claim 11***

The invention recited in independent claim 11 is directed to a system for facilitating authentication services comprising:

an authentication server **(Figure 1)** configured to provide an authentication certificate to a user of a first client device for authentication or identification of a user of

a second client device, the first and second client devices being configured to communicate with each other and the authentication server **(Figure 1, items 28 and 30)**, each of the first and second client devices including a user control program configured to communicate data to and from the authentication server **(page 29, lines 1-9)**, and a media gateway coupled **(Figure 1, items 10 and 11)** to the authentication server and enabling communication of media data from the first and second client devices to the authentication server,

wherein, the user control program of the first client device, in response to a voice command of the first user requesting authentication of the second user, is configured to receive a certificate corresponding to the user of the second client device and the authentication certificate from the authentication server and being configured to authenticate the user of the second client device by comparing the certificate corresponding to the second client device and the authentication certificate **(page 29, lines 10-25, Figure 12)**.

## GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. All claims stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 6,636,975 to Khidekel et al. in view of U.S. Patent 6,668,044 to Schwartz.

## ARGUMENT

***REJECTION UNDER 35 U.S.C. 103(a)***
***Claims 1-20***

Appellants appeal the rejection of all pending claims, which is based on the Examiner's position that the claimed apparatus is obvious in view of Khidekel and Schwartz.

This position reflects a basic misunderstanding and misapplication of patent law and the MPEP, and Appellants submit not only that the claimed apparatus is distinct from that disclosed by the combination of Khidekel and Schwartz, but also that the various phrases and limitations in the claims are to be given patentable weight.

***Independent claim 1 and its dependent claims 2, 4-10 and independent 11 and its dependent claims 12, 14-20:***

Independent claim 1 is method type claim reciting a novel way to identify or authenticate one party on a telephone call to the second party on the call. Similarly, independent claim 11 is a system type claim reciting the novel system which realizes this identification scheme. In both claims, the first party merely speaks a voice command during the telephone call which initiates the identification or authentication process. For example, page 31, line 24 et esq., of the application as filed indicates that the voice command spoken by the first caller may simply be "remote authenticate". That is, during the call, the first caller will simply speak the phrase "remote authenticate" into the phone during the call and the invention will proceed to authenticate the identity of the second party to provide the first party with assurances that they are, in fact, speaking with the person to whom they think they should be speaking.

The Final rejection made by the Examiner relies on the combination of Khidekel and Schwartz. However, as understood, and summarized in the Advisory Action mailed on May 16, 2005, the Examiner seems to rely solely on Schwartz as teaching all of the claimed recitations.

It is respectfully submitted that neither Schwartz alone nor the combination of Schwartz and Khidekel teach or suggest authenticating the identity of a caller during the call, let alone doing so simply by speaking a voice command into the phone during the call.

**Khidekel:**

As understood, Khidekel appears to be directed to a system for securing communications between a client browser and a server over the internet or other network using a secure certificates and a security agent and user biometrics.

As shown in Figure 3, a request for a certificate for authenticity is requested by a browser 204. Indeed, the corresponding passage at column 5, lines 3-4, states "Browser 204 submits a certificate request to certificate authority 214 at 306. The certificate request includes the minutia and identification information. Certificate authority 214 verifies the identification information using conventional methods at 308" (emphasis added).

Thus, Khidekel in no way teaches or suggests allowing one user on a call to verify the other caller's authenticity simply be speaking a dialog voice command as claimed.

In response to the first Office Action in this case, Appellants successfully argued that one party authenticating another party simply by a "voice command" was not taught or suggested by Khidekel.

**Schwartz:**

In the final Office Action, the Examiner further relied on the U.S. Patent 6,668,044 to Schwartz for the teaching of "detecting a voice command from a first caller during the telephone call" (Final Office Action, page 3, lines 2-3). Further, the Examiner has cited to column 9, line 64 to column 10, line 11 of the Swartz reference to support this finding.

However, nothing in the cited to passage, or seemingly anywhere in Schwartz, remotely suggests "detecting a voice command" as alleged by the Examiner and certainly not for the purpose of one party to a call authenticating the other. The relied upon passage in Schwartz states:

"*In one embodiment of the subject invention, the method of recording telephone conversations between two or more parties is employed in conjunction with an Advanced Intelligent Network (AIN). In this instance, the central archiving facility is configured to monitor and record telephone conversations. Accordingly, one or more telephone lines are monitored to detect the initiation or receipt of a telephone call. The content of the telephone call is then recorded by the central archive facility upon initiation or receipt of the call*" (Schwartz column 9, line 64 to column 10, line 11).

This passage merely indicates that a central facility is provided to monitor and record telephone calls. It has absolutely nothing to do with one party authenticating

another party with a "voice command" as claimed. At best, portions of Schwartz may relate to recording and archiving calls by various methods of in-band signaling.

In the Advisory Action, the Examiner insists that Schwartz does indeed teach "*authenticating one party to another using voice commands*". In support of this premise this time, the Examiner states:

"*The telephone lines are monitored to detect the initiation of a telephone call (see col. 10, lines 2-3). The central archive can monitor individuals by using voice recognition patterns (see col. 10, lines 1-12). Further, Schwartz discloses the call may be archived as a means to authenticate the identity of the parties to a conversation (see col. 1, lines 52-56). Thus since Schwartz discloses voice recognition, the Applicant's remarks are moot.*"

However, the Board will please note that nothing in the evidence cited to by the Examiner has anything to do with "authenticating one party to another using voice commands" which is the original premise stated by the Examiner. The Examiner points to unrelated features in Schwartz and then simply concludes at the end that "Thus Schwartz discloses voice recognition". Further, even assuming arguendo that Schwartz does suggest "voice recognition" nothing in either reference remotely suggests that "voice recognition" is in anyway related to speaking a "voice command" to begin an authentication process as recited in the claims.

Further, any "authentication" of the callers that may be done by Schwartz is in the context of archiving. That is, the call is archived, then later authenticated. Archiving

involves recording the call and storing it in an archive for later analysis and verification. Thus, this is absolutely unrelated to allowing one party to speak a voice command to authenticate the other party "during the call", as recited in the claims. Obviously Schwartz's archived authentication is not "during the call".

***Claims 3 and 13***

Dependent claims 3 and 13 recite "monitoring the communication between the first user and the second user so that the authentication server may notify the first user if the second user changes or becomes untrustworthy"

Nothing in either Khidekel or Schwartz teaches or suggests notifying a party to the call that the other party to the call has become untrustworthy during the call.

In the final Office Action, the Examiner relies on Khidekel column 5, lines 37-67 and column 6 lines 1-23. This is indeed a huge section of text relied upon to teach such a short recitation. However, even in all that text, nothing is taught, suggested or implied that a caller level of trustworthiness can be indicated on the fly. Indeed the only thing this passage of Khidekel appears to teach is that a secure server will allow access of a browser requesting access if, for example, the browser was previously authenticated in the past two hours.

This is unrelated to claims 3 and 13 and indeed unrelated to Appellant's entire invention.

Referring to MPEP § 2143, titled "Basic Requirements for a Prima Facie case of

Obviousness", the MPEP mandates that:

"To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claimed limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not applicant's disclosure." (emphasis added).

It is again respectfully submitted that all of the features, recited in the claims as discussed above, are not present even if Khidekel and Schwartz are combined. Thus, the combination does not make a case for *prima facie* obviousness under § 103.

It is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. In re Fine, 837 F.2d 1071, 5 U.S.P.Q. 2d 1596 (Fed. Cir. 1988). This objective can only be established by an objective teaching in the prior art or by cogent reasoning that the knowledge is available to one of ordinary skill in the art. In re Lalu, 747 F.2d 703, 223 U.S.P.Q. 1257 (Fed. Cir. 1988). Here there is none.

Indeed, in the case at hand, the Examiner has failed to disregard what he has been taught by the present invention and has failed to cast his mind back to the time that the invention was made to determine what would have been obvious to one ordinarily skilled in the art who had available only the references and the then-accepted wisdom in the art.

Assuming arguendo that Khidekel and Schwartz could be interpreted in the manner suggested by the Examiner, the rejection would still be insufficient since as a matter of fact both Khidekel and Schwartz fail to teach the above highlighted claim recitations.

The PTO has the initial burden under section 103 to establish a *prima facie* case of obviousness. See, In re Piasecki, 223 USPQ 785, 788; In re Fine, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). The PTO can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references, Ashland Oil, Inc. V. Delta Resins & Refractories, Inc., 776 F.2d 281, 297 n.24, 227 USPQ 657, 667 n.24 (Fed. Cir. 1985); ACS Hosp. Sys., Inc. v. Monteviore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). Here, it is respectfully submitted that the Examiner has failed to show *prima facie* obviousness.

As such, it is respectfully requested that the Board reverse the Examiner and allow all claims.

## CONCLUSION

In summary, Khidekel and Schwartz do not teach or suggest the features of the claimed invention. Therefore, the references do not provide evidence that would support a conclusion of obviousness under 35 U.S.C. §103(a). Appellants thus respectfully submit that the rejections of claims 1-20 are in error and that reversal is warranted in this case.

Respectfully submitted,

/Kevin A. Reif/

Kevin A. Reif
Reg. No. 36,381

INTEL
LF1-102
4050 Lafayette Center Drive
Chantilly, Virginia 20151
(703) 633-6834

## CLAIMS APPENDIX

A copy of the claims involved in the appeal is provided below.

1 (previously amended). A method for providing authentication or identification services to a first user regarding a second user, the method comprising:

establishing a telephone call between the first user and the second user through a media gateway;

detecting a voice command from the first caller during the telephone call;

requesting a certificate corresponding to the second user from an authentication server in response to the voice command;

returning the certificate corresponding to the second user;

requesting authentication of the certificate corresponding to the second user from a control program associated with the second user;

returning an authentication certificate from the control program associated with the second user; and

verifying authentication by comparing the authentication certificate corresponding to the second user and received from the control program associated with the second user with the certificate received from the authentication server.

2 (original). The method according to claim 1, wherein the first user communicates with the second user through a media gateway.

3 (original). The method according to claim 1, further comprising monitoring the communication between the first user and the second user so that the authentication server may notify the first user if the second user changes or becomes untrustworthy.

4 (original). The method according to claim 1, wherein the requesting of the certificate corresponding to the second user from the authentication server, requesting authentication of the certificate corresponding to the second user and the verifying authentication is performed by a control program associated with the first user.

5 (original). The method according to claim 1, wherein the first and second users are using client devices configured to communicate with each other and with the authentication server.

6 (original). The method according to claim 5, wherein the client devices are smart phones.

7 (original). The method according to claim 1, wherein the authentication server has authenticated an organization and the second user is a member of the authenticated organization.

8 (original). The method according to claim 1, wherein verifying authentication determines a level of trust between the first user, the authentication server and the second user.

9 (original). The method according to claim 8, wherein the level of trust is a value corresponding to the probability that the authentication certificate corresponding to the second user and received from the control program associated with the second user is the same as the certificate received from the authentication server.

10 (original). The method according to claim 1, wherein the authentication certificate corresponding to the second user and received from the control program associated with the second user includes a portion indicating the second user's identity.

11 (previously amended). A system for facilitating authentication services comprising:

an authentication server configured to provide an authentication certificate to a user of a first client device for authentication or identification of a user of a second client device, the first and second client devices being configured to communicate with each other and the authentication server, each of the first and second client devices including a user control program configured to communicate data to and from the authentication server, and a media gateway coupled to the authentication server and enabling communication of media data from the first and second client devices to the authentication server,

wherein, the user control program of the first client device, in response to a voice command of the first user requesting authentication of the second user, is configured to receive a certificate corresponding to the user of the second client device and the

authentication certificate from the authentication server and being configured to authenticate the user of the second client device by comparing the certificate corresponding to the second client device and the authentication certificate.

12 (original). The system according to claim 11, wherein the authentication server is configured to monitor the communication between the first user and the second user.

13 (original). The system according to claim 11, wherein the authentication server is configured to continuously monitor the communication between the first user and the second user so as to notify the first user if the second user changes or becomes untrustworthy.

14 (original). The method according to claim 11, wherein the control program associated with the first user is configured to request the certificate corresponding to the second user from the authentication server, request authentication of the certificate corresponding to the second user and verify authentication.

15 (previously amended). The system according to claim 11, wherein the first and second users use client devices configured to communicate with each other and with the authentication server.

16 (original). The system according to claim 15, wherein the client devices are smart phones.

17 (original). The system according to claim 11, wherein the authentication server has authenticated an organization and the second user is a member of the authenticated organization.

18 (original). The system according to claim 14, wherein verifying authentication determines a level of trust between the first user, the authentication server and the second user.

19 (original). The system according to claim 18, wherein the level of trust is a value corresponding to the probability that the authentication certificate corresponding to the second user and received from the control program associated with the second user is the same as the certificate received from the authentication server.

20 (original). The system according to claim 11, wherein the authentication certificate corresponding to the second user and received from the control program associated with the second user includes a portion indicating the second user's identity.

21-47 (cancelled).

## EVIDENCE APPENDIX

This section lists evidence submitted pursuant to 35 U.S.C. §§1.130, 1.131, or 1.132, or any other evidence entered by the Examiner and relied upon by Appellant in this appeal, and provides for each piece of evidence a brief statement setting forth where in the record that evidence was entered by the Examiner. Copies of each piece of evidence are provided as required by 35 U.S.C. §41.37(c)(ix).

| NO. | EVIDENCE | BRIEF STATEMENT SETTING FORTH WHERE IN THE RECORD THE EVIDENCE WAS ENTERED BY THE EXAMINER |
|---|---|---|
| 1 | N/A | N/A |

## RELATED PROCEEDINGS APPENDIX

Pursuant to 35 U.S.C. §41.37(c)(x), copies of the following decisions rendered by a court of the Board in any proceeding identified above under 35 U.S.C. §41.37(c)(1)(ii) are enclosed herewith.

| NO. | TYPE OF PROCEEDING | REFERENCE NO. | DATE |
|---|---|---|---|
| 1 | N/A | N/A | N/A |